International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

# A Survey on Distributed Database System Security Approaches

**Gebrearegawi Gebremariam** [1]

Lecturer at Faculty of Computing Technology, Aksum Institute of Technology, Aksum University, Aksum, Tigray, Ethiopia[1]

**ABSTRACT**: As distributed database systems became more popular, the need for improvement of distributed database management system becomes even more significant. Among these needs, the most important enhancement is developing a secured and trusted database in a distributed systems environment that may arise and possibly compromise controlled and confidential system. The main purpose of this study is to understand the different security threats that encounter for database system designed in a distributed environment and the different security mechanisms to countermeasure these problems. Several security approaches for distributed database systems have been discussed, like authentication, cryptography, trust-based models, access control-based approaches, etc. to build confidential, authenticated, reliable, and available distributed database system.

**KEYWORDS**: Distributed Systems, Distributed Database system, Security, Confidentiality, Authentication, Access Control, Cryptography, Trust

## I. INTRODUCTION

As known, networks of computers are everywhere at this time. Thus, computers rarely work in isolation in today's networked world means that computers collaborate with each other for the purpose of data communication, processing, transferring, storing etc. This collaboration plays an important role in developing new era of information technology called Distributed Systems. A collection of multiple and heterogeneous machines systems which are physically distributed across various locations and communicate via a network is referred to as Distributed Systems [1]. These machines in a distributed system are interconnected to each other either through wireless connection or through various communication media that serve data transfer at high rate.

The objectives of building distributed systems are achieving service transparency, openness, reliability, performance, and scalability [2]. And the most important part of distributed systems is its joint data network which is the nerve center of organizations and tends to grow with the development of the organizations and the development of technology [3].

A distributed database system is a type of distributed system which is composed of multiple logically interrelated databases and located physically across various locations that communicate via a computer network. Here, the computers collaboratively store data in such a manner that a user can access data from anywhere as if it has been stored locally irrespective of where the data is actually stored. Since data is the most valuable asset of any organization, securing the data is one of the most important focuses and wishes for every governmental and private organization. But, before applying security mechanisms, the organizations should know the possible security threats and attacks for the distributed database systems. As stated in [6], [7], distributed database has number of security challenges and threats.

## II. DISTRIBUTED DATABASE SECURITY CHALLENGES

### I. System Complexity:

To provide anacceptable level of performance, reliability, availability is inherently and to hide the distributed nature from the user in a distributed databasesystems is more complex. In addition, the data replication across multiple locations adds an extra level of complexity to the distributed DBMS. There will be degradation in availability, reliability and performance compared with the centralized system if the software does not handle data replication adequately. As a result, the advantages described above become disadvantages.

### II. Increased Cost:

Increased complexity means that we can expect the procurement and maintenance costs for a DDBMS to be higher than those for a centralized DBMS. Furthermore, a distributed DBMS requires additional hardware to establish a

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

network between sites. There are ongoing communication costs incurred with the use of this network. There are also additional labor costs to manage and maintain the local DBMSs and the underlying network.

**III. Vulnerability to Attack:**

In a centralized system, access to the data can be easily controlled. However, in a distributed database system not only the accessibility to replicated data has to be controlled from multiple locations but also the network itself has to be made secure using significant security protocols both to the networks and to the data.

## III. DISTRIBUTED DATABASE SYSTEM SECURITY THREATS

As stated by Bhargava& Lilien (2014), the distributed system threats could be classified according to their actions and consequences. Their actions include observing, modifying, destroying, and emulating the data and their consequences can be activities like disclosing, executing, misrepresenting, and repudiating threats [7][2]. These security threats and attacks may be one of the following:

1. **Input Injection (SQL Injection):** is an attack in which an attacker introduces malicious codes with the standard SQL codes to get informed about the sensitive information from secure databases**.** There are two common types of database injection attacks: 1) SQL Injection that targets the traditional database systems and 2) NoSQL Injection that targets Big Data platforms. In both types, a successful Input Injection attack can give an attacker unrestricted access to the entire database [8].
2. **Distributed Denial of Service (**DDoS) is a general attack category in which access to network applications or data is denied to intended users. In Distributed Denial of Service Attacks (DDoS), attackers send a huge number of requests coordinated from many locations simultaneously, thus the actual service become unavailable to the trusted users. The motivations behind DDoS attacks are often linked to extortion scams in which a remote attacker will repeatedly crash servers until the victim meets their demands. Whatever the source, DDoS represents a serious threat for many organizations [2].
3. **Weak Audit Trail:** Thisis automated recording of database transactions involving sensitive data should be part of any database deployment.
4. **Storage Media Exposure:** This may happen when numerous security breaches have involved the theft of database backup disks and tapes because backup storage media is often completely unprotected from attack. Furthermore, our data lays at risk if there is failure to audit and monitor the activities of administrators who have low-level access to sensitive information.
5. **Message tampering (Interception):** is the process of getting message and altering their contents before passing on to the intended recipient. The man-in-the-middle attack is a form of message tampering in which an attacker intercepts the sensitive message contents in an exchange of encryption keys to establish a secure channel with intended recipient [9].
6. **Masquerading (Phishing):** is a form of attack in which an attacker sends or receives messages using the identity of another recipient without authority [9].
7. **Sniffing**: This is the process where an attacker monitors the data travelling from sender to receiver across the network.

There are also other security threats such as inference and Identity theft [3], [8], [10], [11].The inference threat may be caused through data mining i.e. when a user makes various data queries.

8. The impersonation or misuse of identity, modifying access control structures, repudiating of a principal participating in a protocol, destruction or modification of programs or data, leakage of information and traffic analysis are identified as the main types of security threats in distributed systems [12].

As a result, in order to have a well-developed and secured distributed database system, researchers should study the sources of these challenges and ways of assuring security to the system. Hence, the main aim of this study is to discuss the security challenges and attacks of distributed database systems and their countermeasure mechanisms to protect data.

## IV. DISTRIBUTED DATABASE SYSTEM SECURITY APPROACHES

Several security approaches have been proposed by different researchers to handle the security and privacy of data stored in distributed database systems. These security approaches may vary to the different types of distributed systems [10][15][4]. Accordingly, there are different security approaches of distributed database systems. These approaches can be broadly categorized as the following:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

### A. Authentication-Based Security Approaches

In order to authenticate users before accessing the system, several authentication methods are stated by many computing scholars. One of these authentication approaches is password-based authentication. Most organizations use this authentication method. However, this is unsatisfactory because the protocol is asymmetric in its trust as stated in [16]. For this purpose, he introduced a trusted third party called Authentication Server to provide confidentiality, authenticity and to know identity of messages sent from one site to another [16]. A path authentication is also proposed in [10][12] to discover paths with secured domains in a distributed environment.

Furthermore, a three-factor authentication approach is another security mechanism identified in [10], [15] to confirm remote client in the distributed systems environments. These authentication factors are password, smart-card and biometrics. Biometric authentication systems consist of two stages: the enrollment and authentication /identification stages. Biometric authentication is better than password authentication. However, Biometric authentication can face a replay attack [17], [18]

### B. Access Control-Based Security

Access controls are security approaches that control how users and systems communicate and interact with other systems and resources based on the security policy of the organization [14]. Access is controlled by classifying elements of the database. The basic element of this classification is the object. Access permission is granted if the user has sufficient security clearance to access the methods of an object [19].

Role-based access control (RBAC) is used to solve the problem of managing authorization in the growth of intranet web servers according to role hierarchies because if there are large number of users or permission associations on all servers there is greater risk of maintaining residual and inappropriate user access rights. However, with RBAC permissions are authorized to roles and roles are authorized to users. According to Kuhn, et al (1999), RBAC has two components: $MC_0$ and $MC_1$. $MC_0$ is also calledRBAC authorization database model describes the authorization into static roles. $MC_1$ is also called RBAC Activation model describes the RBAC security properties for dynamic activation properties [20], [21].

### C. Trust-Based Security Approaches

Trust is defined as the requirements for making decision on communication between entities i.e. the state of accepting vulnerabilities as a positive expectations [22]. Trust-based security method is introduced to increase authentication, access control, secure service provision, and secure routing in various applications. Hence, the main aim of trust is to check valid user identities at each system levels. For effective trust-based access control, service-oriented access control, privacy preserving, revocation of invalid ongoing access and filtering malicious recommendations from competitors are the most determinant points. According to Prakash & Darbari (2014), trust management can be divided into two kinds; Rule-base system andReputation system [23]. There are different trust-based security provision methods such as password-based authentication and authorization of users, Kerberos-based messages encryption based on symmetric key cryptography [10].

Furthermore, the common distributed trust models are Simple Public key Infrastructure (SPKI), Pretty Good Privacy (PGP), and Matt Blaze's Policy Maker. SPKI is used for authentication and authorization. An entity PGP is trusted when one or more trusted entities say that it can be trusted. Policy-Maker is a model which binds public keys to access control without authentication [21]. Trust-based distributed database systems security should be highly capable of dealing with the security attacks in all aspects [23].

### D. Cryptography-Based Security Approaches

According to Herlihy & Tygar (1987), there are two notions of cryptographic security: bit-security and perfect security. Bit-security implies that given cipher-text, no processor with randomized polynomial resources can derive information about any given bit in the corresponding clear-text with certainty greater than $1/2+\varepsilon$ for any $\varepsilon > 0$. RSA cryptosystem is bit-secure under the assumption that taking thk roots modulo pq, a product of two large primes, cannot be done in randomized polynomial time and that the Rabin signature schemes is bit-secure if factorization is not in randomized polynomial time.

Perfect security on the other hand implies that given cipher-text, no processor with unlimited resources can derive a probability distribution of the corresponding clear-text other than a uniform distribution [1].

DNA-based cryptography approach together with a rule-based post processing approach has been suggested to prevent attacks in the distributed database systems in [10].

### E. Policy-based Security Approaches

The policy-based security approach has been proposed in [15] to provide modular security system and independent underlying systems. Different access control policy models are also proposed such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) [24]. A policy based distributed system security mechanism based on domain language for verification has been also described to implement security for distributed database system[10].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

### F. Pattern-based Security Approaches

The Pattern is a security mechanism to control some security threats in several levels of abstraction [22][9]. The model of firewall patterns hierarchy is described in [22]. There are four basic types of firewalls, which filter at different architectural levels: The Application (User level) Firewall, the Proxy Firewall (system application), the Stateful Firewall, and the Packet Filter Firewall. Other types of patterns based on levels of abstraction, concerns, and relationships have been also described in [22]. These are application level firewalls, XML firewalls, Proxy Firewalls, Packet Filter Firewalls.

### G. Quorum-based Security Approaches

Quorum replication is an important method for creating distributed systems to simultaneously improve both the integrity and availability of computation and storage [25]. The quorum-based security is used to solve the problem of data inconsistency in distributed fault tolerance systems [15]. In addition, a security typed language, Qimp, has been proposed in [25] to provide an end-to-end security assurance of quorum replication system protocols from interference. Qimp is a simple imperative language designed for the common distributed computing systems in which the client machine may use a set of server hosts to store data and perform computations. The private-key Secure Quorum Consensus (SQC) protocol with three phases (Object initialization, Front-end initialization, Operation Execution) is stated to provide a single key for both encryption and decryption. Public key Secure Quorum Consensus (SQC) protocol is also stated that uses public key ($K_E$) for encryption and private key ($K_D$) for decryption [1].

### H. Perimeter-Based Security

Another security approach, Perimeter-Based Security (also called network-based Security systems) approach is used to intercept the communication between clients and servers and cross-examine that traffic for accepting with established security policies within them. Firewalls and IPSs are the common examples of Perimeter-Based Security approach. There are four basic types of firewalls, which filter at different architectural levels: the Application (User level) Firewall, the Proxy Firewall (system application), the Stateful Firewall, and the Packet Filter Firewall [9].
The common advantage of these security methods is their coverage. Wherever the computing systems are located and whatever computing system devices can be protected by using firewalls.However, perimeter-based Security approaches can be challenged by even more fundamental problems. When workloads are dynamically created, moved, and decommissioned, all on demand, it becomes impossible to define a perimeter in the traditional sense.

### I. Host-Based Security Approaches

Host-based security approach involves running a piece of security software program on the same operating system running the client or server application. Antivirus software, which is the best example for host-based security, has the benefit of installing on the endpoint to protect and simplify workload mobility challenges.

### J. Other Security Approaches

Image-based challenge/response method and WSQ-based data hiding are proposed as a solution to the replay attack in biometric system [18]. Intrusion-Tolerance Quorum System has been discussed in [10] to solve data inconsistency problem in Distributed Database systems. CORBA based authentication security model has also discussed in [10]. Layering of Security mechanism in distributed system has been discussed in [2] to enhance the security of the system.

## V. CONCLUSION

This study provides a conceptual framework about the possible threats of distributed database security and different techniques of securing the system like Authentication, access control, cryptographic, trust-based models and many others which can be helpful towards the generation of secure and trusted distributed database systems. Generally, it is seen that most of the studies target specific areas of security attacks and security mechanisms. Detecting and protecting security threats and attacksof distributed databasesystems must be critical issue of organization for the accurate identification of advanced attackers moving laterally across physical, virtual, and cloud assets across the data in a distributed environment. Lastly, it is expected that rapid growth of the new systems with distributed database systems should be careful about the security of the database in all aspects.

## REFERENCES

[1]M. P. Herlihy and J. D. Tygar, “How to Make Replicated Data Secure?,” in Conference on the Theory and Application of Cryptographic Techniques, 1987, no. August, p. 11.
[2]A. Tanenboun, Distributed System principles and paradigms, Second edi. Amsterdam: Vriji University, 2006.
[3]A. Armoni, “Data Security Management in Distributed Computer Systems,” Informing Sci., vol. 5, no. 1, 2002.
[4]M. Firdhous, “Implementation of Security in Distributed Systems – A Comparative Study,” Int. J. Comput. Inf. Syst., vol. 2, no. 2, pp. 1–6, 2011.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

[5]D. Harinath and P. Satyanarayana, "A Review on Security Issues and Attacks in Distributed Systems," J. Adv. Inf. Technol., vol. 8, no. 1, pp. 1–9, 2017.
[6]D. S. Hiremath and S. B. Kishor, "Distributed Database Problem areas and Approaches," in National Conference on Recent Trends in Computer Science and Information Technology, 2016, pp. 15–18.
[7]B. Bhargava and L. Lilien, "Vulnerabilities and Threats in Distributed Systems," West Lafayette, 2014.
[8]S. Pal, N. Chaki, S. Sanyal, and S. Khatua, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security," 2011, p. 31.
[9]R. Kumari and K. Singh, "Partial Security Violation Model in Non-Blocking Distributed Databases," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 12, pp. 283–289, 2012.
[10]P. Singh and K. Rai, "An overview of different database security approaches for distributed environment," Int. J. Innov. Sci. Eng. Technol., vol. 2, no. 6, pp. 316–321, 2015.
[11]İ. Köse, "Distributed Database Security," GYTE, 2002.
[12]L. O. Connor, G. Gaskell, and W. J. Caelli, "Security Issues in Distributed Computing," Australia, 2014.
[13]J. D. Moffett, "Security & distributed systems," UNIVERSITY OF YORK, 1990.
[14]R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia - Procedia Comput. Sci., vol. 48, no. Iccc, pp. 204–209, 2015.
[15]V. Prakash and M. Darbari, "A Review on Security Issues in Distributed Systems," Int. J. Sci. Eng. Res., vol. 3, no. 9, pp. 1–5, 2012.
[16]T. Quasim, "Security Issues in Distributed Database System Model," An Int. J. Adv. Comput. Technol., vol. 2, no. Xii, pp. 396–399, 2013.
[17]E. Maiorana and C. Ercole, "Secure Biometric Authentication System Architecture using Error Correcting Codes and Distributed Cryptography," in Conference GTT, 2007, p. 12.
[18]N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," in Proc. Int. Conf. Audio and Video-based Biometric Person Authentication, 2001, p. 13.
[19]S. Kumar, J. Seetha, and R. Vinotha, "Security Implications of Distributed Database Management," Int. J. Soft Comput. Softw. Eng., vol. 2, no. Nov 25, pp. 20–28, 2012.
[20]R. Kuhn, "A Role Based Access Control Model and Reference Implementation within a Corporate Intranet," A C M Trans. Inf. Syst. Secur., no. October 2015, 1999.
[21]L. Kagal, T. Finin, and A. Joshi, "Trust-Based Security in Pervasive Environments," in IBM EECOMS, 2001, p. 5.
[22]E. B. Fernandez, J. Jurjens, and M. Vanhilst, "Using Security Patterns to Develop Secure Systems," Int. J. Syst. Softw. Secur. Prot., vol. 9, no. 4, pp. 16–31, 2018.
[23]V. Prakash and M. Darbari, "A New Framework of Distributed System Security Using DNA Cryptography and Trust Based Approach," Int. J. Adv. Res. Technol., vol. 3, no. 3, pp. 1–4, 2014.
[24]J. Fisher, "Top Ten Database Security Threats The Most Significant Risks of 2015 and How to Mitigate Them.," Cyber Security & Data Protectice, 2015. .
[25]L. Zheng and A. C. Myers, "A Language-Based Approach to Secure Quorum Replication," in Proceedings of the Ninth Workshop on Programming Languages and Analysis for Security, 2014, p. 13.